



TITLE:

量子i.i.d.状態の数値シミュレーション: 仮説検定を題材にして (量子論における統計的推測の理論と応用)

AUTHOR(S):

坂下, 達哉

---

CITATION:

坂下, 達哉. 量子i.i.d.状態の数値シミュレーション: 仮説検定を題材にして (量子論における統計的推測の理論と応用). 数理解析研究所講究録 2013, 1834: 77-88

ISSUE DATE:

2013-05

URL:

<http://hdl.handle.net/2433/194882>

RIGHT:

# 量子 i.i.d. 状態の数値シミュレーション — 仮説検定を題材にして

東京大学・物性研究所 坂下 達哉

Tatsuya Sakashita

Institute for Solid State Physics, The University of Tokyo

## 1 はじめに

量子情報理論を理解する上で、量子 i.i.d. 状態 ( $n$  次テンソル積で表される状態) に関する漸近的性質が重要である。これまで、古典情報理論において漸近性を研究する上で、各種の数値的手法が活用されてきた。一方、量子情報理論においては、このような手法が実現可能とも有効であるとも考えられていなかった。

テンソル積の既約分解は群の表現論における基本的概念の一つであり、林 [1] によって量子 i.i.d. 状態の漸近性の研究に導入されて以来、量子情報理論における重要な数学的手段となっている。長岡は、テンソル積の既約分解が量子 i.i.d. 状態に関する数値シミュレーション手法として有効であることを見だし、文献 [2] において、 $2 \times 2$  の密度行列からなる i.i.d. 状態の仮説検定の誤り確率について  $n = 50$  の場合までの計算例を示した。このアイデアは、長岡の指導のもと、柿崎 [3]、堂嶋 [4] によって検討され、後者では  $n = 300$  までの計算例が示された。

本研究の目的は、この手法を用いて、既知の量子仮説検定の定理を題材として大規模な次数  $n$  について高精度の数値シミュレーションが可能であることを実証することである [5–10]。また、このように既知の定理を利用して確立した数値的手法を新しい問題の漸近的性質の数値的検証に活用することである。例えば、文献 [5, 9, 10] では、中心極限定理に関連した新しい予想を数値的に検証している。

本稿では、以上の成果を統計学、物理的側面に焦点を当てて概要を述べる。本稿の構成は以下のとおりである。2 節および 3 節では、本稿で用いる量子力学の最小限の事柄を述べた後、量子 i.i.d. 状態の定義を行う。4 節では、二つの量子 i.i.d. 状態に対する仮説検定を紹介する。5 節では、 $n \rightarrow \infty$  のときの量子仮説検定の漸近論について述べる。5 節の目標は、数値計算の題材とする量子 Hoeffding の定理を説明することである。6 節で  $2 \times 2$  行列のテンソル積の既約分解について述べ、これを適用した誤り確率の計算手法を 7 節で記述する。この計算手法を確立するために量子 Hoeffding の定理の数値的検証を行った結果を 8 節で述べる。9 節では、中心極限定理に関連した新しい予想の問題設定を述べ、上記の計算手法を用いて予想の数値的検証を行う。10 節をまとめとする。

## 2 量子力学の基礎

本節では、線形代数の知識のみを仮定し、量子力学について記述する。

量子力学は Hilbert 空間 (完備な内積  $\langle \cdot | \cdot \rangle$  を持つ線型空間) 上の作用素を用いて記述される。本稿では有限次元の場合しか扱わないので、Hilbert 空間を自然内積を持つ複素数ベクトル空間

$$\mathbb{C}^d := \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix} \mid a_i \in \mathbb{C} \quad (i = 1, \dots, d) \right\}$$

と同一視する。また、作用素も  $d \times d$  サイズの複素数成分の正方行列と考えて良い。自然内積の定義は、 $\mathbb{C}^d$

の元

$$\psi = \begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix}, \quad \phi = \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix}$$

に対して,

$$\langle \psi | \phi \rangle := \psi^* \phi = \sum_{i=1}^d \bar{a}_i b_i \quad (1)$$

である。ただし、 $*$  はエルミート共役 (共役転置) を、 $\bar{\phantom{x}}$  は複素共役を表す。式 (1) にあるように、量子力学では縦ベクトル、横ベクトルをそれぞれケット、ブラと呼び次のような記法で表す:

$$|\psi\rangle := \psi = \begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix}, \quad \langle\psi| := \psi^* = [\bar{a}_1 \quad \cdots \quad \bar{a}_d].$$

本稿でも、この記法を用いることにする。

いくつかの物理的な概念に数学的な定義を与える。量子状態は、トレースが 1 の半正定値行列 (密度行列と呼ばれる)  $\rho$  で表される。測定は、半正定値行列の集合  $M = \{M(x)\}_{x \in \mathcal{X}}$  で、 $\sum_{x \in \mathcal{X}} M(x) = I$  (単位行列) を満たすもので表される。これを POVM (Positive Operator-Valued Measure) と呼ぶ。ここで、添字  $x$  は測定値を表す。量子状態  $\rho$  のもとで測定  $M$  を行ったら、測定値  $x$  が得られる確率は

$$P_\rho^M(x) := \text{Tr}[\rho M(x)] \quad (2)$$

で表される。以上の状況を図 1 に図示する。

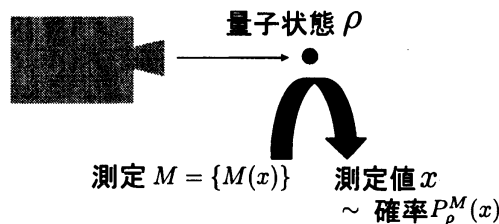


図 1 量子力学における測定

特に、測定  $M = \{M(x)\}_{x \in \mathcal{X}}$  において、

$$M(x)^2 = M(x), \quad M(x)M(x') = 0 \quad (x, x' \in \mathcal{X} \text{ and } x \neq x') \quad (3)$$

が成立するとき  $M$  を単純測定であるという。このとき、各  $M(x)$  は射影子である。例えば、 $d$  次元 Hilbert 空間  $\mathcal{H}$  の正規直交基底  $\{u_i\}_{i=1}^d$  に対して、各  $\{u_i\}$  の張る空間への射影子を  $M(i) := |u_i\rangle \langle u_i| = u_i u_i^*$  とおくと、 $M := \{M(i)\}_{i=1}^d$  は単純測定になっている。このとき、 $M$  を完全測定と呼ぶ。量子状態  $\rho$  に対して、完全測定  $M$  を行ったら、測定値  $i$  が得られる確率は

$$P_\rho^M(i) = \langle u_i | \rho u_i \rangle = u_i^* \rho u_i \quad (4)$$

と表される。特に、密度行列  $\rho$  の固有値を  $\{p_i\}_{i=1}^d$  とし、 $\rho$  の固有ベクトルからなる正規直交基底  $\{u_i\}_{i=1}^d$  に対して  $M(i) := |u_i\rangle \langle u_i|$  によって完全測定  $M := \{M(i)\}_{i=1}^d$  を構成した場合には、

$$P_\rho^M(i) = p_i \quad (5)$$

である。

### 3 合成系と量子 i.i.d. 状態

本節では、量子力学における合成系の数学的表現について紹介し、量子 i.i.d. 状態を定義する。

量子系がいくつか与えられたとき、それらをまとめて一つの系と考えることができる。このような系を合成系とよぶ。いま、 $n$  個の量子系を考える。各量子系を表現する Hilbert 空間を  $\mathcal{H}_i$  とする。この  $n$  個の量子系を表現する Hilbert 空間はテンソル積空間  $\tilde{H} := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$  である。各  $\mathcal{H}_i$  が  $\mathcal{H}_i = \mathbb{C}^{d_i}$  の場合には、 $\tilde{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n = \mathbb{C}^{d_1 \cdots d_n}$  となる。

合成系の状態は、各系の状態と同様に密度行列で表される。特に、各系が独立に  $\rho_1, \dots, \rho_n$  という状態におかれているという状況は、 $\tilde{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$  上の状態  $\rho_1 \otimes \cdots \otimes \rho_n$  で表される。ここで、行列  $A: d \times d$  サイズと  $B: d' \times d'$  サイズのテンソル積を

$$A \otimes B := \begin{bmatrix} a_{11}B & \cdots & a_{1d}B \\ \vdots & \ddots & \vdots \\ a_{d1}B & \cdots & a_{dd}B \end{bmatrix} : dd' \times dd' \text{ サイズ} \quad (6)$$

と定義する。式 (6) より実際に、 $\rho_1 \otimes \cdots \otimes \rho_n$  が量子状態の定義を満たしていることを確かめることができる。

さらに、 $n$  個の量子系が独立に同じ状態  $\rho$  に置かれているという場合、合成系の状態は  $\rho$  の  $n$  次テンソル積  $\rho^{\otimes n} = \rho \otimes \cdots \otimes \rho$  で表される。この状態を量子 i.i.d. (**i**ndependent and **i**dentically **d**istributed) 状態という。ただし、 $\rho$  の行列サイズを  $d \times d$  とすると  $\rho^{\otimes n}$  の行列サイズは  $d^n \times d^n$  である。ここで、 $n$  をテンソル次数と呼ぶ。

古典確率論において、量子 i.i.d. 状態はデータ数  $n$  の独立同一分布に相当する。ここで、 $X^n = (X_1, \dots, X_n)$  を同じ標本集合  $\mathcal{X}$  上の  $n$  個の確率変数の組とする。各  $X_i$  が独立に  $\mathcal{X}$  上の同じ確率分布  $p$  にしたがっているとき、 $X^n = (X_1, \dots, X_n)$  は独立同一に確率分布  $p$  にしたがうという。このとき、 $X^n$  がしたがう  $\mathcal{X}^n := \mathcal{X} \times \cdots \times \mathcal{X}$  上の確率分布

$$p^n(x^n) = p(x_1) \cdots p(x_n) \quad \text{where } x^n = (x_1, \dots, x_n) \in \mathcal{X}^n$$

を独立同一分布と呼ぶ。

合成系の測定は、テンソル積空間  $\tilde{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$  上の POVM で表される。特に、 $M_i = \{M_i(x_i)\}_{x_i \in \mathcal{X}_i}$  を  $\mathcal{H}_i$  上の POVM とすると、 $\tilde{M} := M_1 \otimes \cdots \otimes M_n := \{M_1(x_1) \otimes \cdots \otimes M_n(x_n)\}_{x_1 \in \mathcal{X}_1, \dots, x_n \in \mathcal{X}_n}$  は  $\tilde{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$  上の POVM になる。このとき、

$$P_{\rho_1 \otimes \cdots \otimes \rho_n}^{M_1 \otimes \cdots \otimes M_n}(x_1, \dots, x_n) = \text{Tr}[(\rho_1 \otimes \cdots \otimes \rho_n)(M_1(x_1) \otimes \cdots \otimes M_n(x_n))] \quad (7)$$

$$= \text{Tr}[\rho_1 M_1(x_1)] \cdots \text{Tr}[\rho_n M_n(x_n)] \quad (8)$$

$$= P_{\rho_1}^{M_1}(x_1) \cdots P_{\rho_n}^{M_n}(x_n) \quad (9)$$

が成り立つ。ここで、式 (7) から式 (8) への変形には

$$(A \otimes B)(C \otimes D) = AC \otimes BD \quad (10)$$

$$\text{Tr}[A \otimes B] = \text{Tr}[A] \text{Tr}[B] \quad (11)$$

を用いた。式 (9) は、各系に対して個別に測定  $M_i$  を行うことと、合成系に対して測定  $\tilde{M} = M_1 \otimes \cdots \otimes M_n$  を行うことは同等であることを意味する。

本稿では、量子状態としては量子 i.i.d. 状態、測定としては POVM をなす各正定値行列がテンソル積で表せない場合が重要である。また、量子 i.i.d. 状態  $\rho^{\otimes n}$  を考える際には、密度行列  $\rho$  は物理的に興味のある個々の例ではなく、一般の密度行列  $\rho$  とする。一般の密度行列  $\rho$  に対する量子 i.i.d. 状態  $\rho^{\otimes n}$  についての数学的な問題設定を考えることにする。

#### 4 量子 i.i.d. 状態とその仮説検定

本節では、量子 i.i.d. 状態の定義、二つの量子 i.i.d. 状態に対する仮説検定の問題設定について述べる。[2].

今、二つの量子 i.i.d. 状態  $\rho^{\otimes n}, \sigma^{\otimes n}$  のうちどちらかが与えられているとして、何らかの測定を用いて真の量子状態がどちらであるかを判定する問題を考える。判定結果が「 $\rho^{\otimes n}$  である」「 $\sigma^{\otimes n}$  である」という事象をそれぞれ 0, 1 で表すことにし、判定のプロセスは二値測定を表す POVM  $M^n = \{M^n(0), M^n(1)\}$  で与える。ただし、 $M^n(0), M^n(1)$  は、 $\rho^{\otimes n}, \sigma^{\otimes n}$  と同じサイズの半正定値行列である。以上の判定のプロセスを図 2 に図示する。

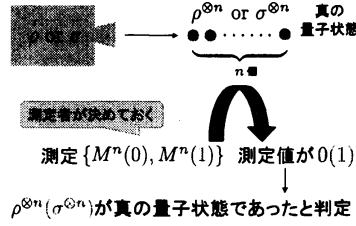


図 2 量子仮説検定:  $\rho^{\otimes n}$  v.s.  $\sigma^{\otimes n}$

真の状態	測定値	判定	正・誤
$\rho^{\otimes n}$	0	$\rho^{\otimes n}$	正しい
	1	$\sigma^{\otimes n}$	第 1 種誤り
$\sigma^{\otimes n}$	0	$\rho^{\otimes n}$	第 2 種誤り
	1	$\sigma^{\otimes n}$	正しい

図 3 量子仮説検定における誤り

以上の判定方法では、 $\rho^{\otimes n}$  が真であるが  $\sigma^{\otimes n}$  が真と判定する誤りと、 $\sigma^{\otimes n}$  が真であるが  $\rho^{\otimes n}$  が真と判定する誤りが生じ得る。これらをそれぞれ第 1 種・第 2 種誤りと呼ぶ。この状況を図 3 に示す。

POVM  $M^n = \{M^n(0), M^n(1)\}$  において  $M^n(0) + M^n(1) = I_n$  が成り立つので、 $M^n$  を一つの行列  $T_n := M^n(0)$  で指定することができる。この  $T_n$  を検定と呼ぶ。検定を用いてこれらの誤りが生じる確率を表すと、

$$\alpha_n[T_n] := \text{Tr}[\rho^{\otimes n}(I - T_n)] = 1 - \text{Tr}[\rho^{\otimes n}T_n] \quad (12)$$

$$\beta_n[T_n] := \text{Tr}[\sigma^{\otimes n}T_n] \quad (13)$$

となる。ここで、 $\alpha_n[T_n], \beta_n[T_n]$  はそれぞれ第 1 種・第 2 種誤り確率と呼ばれる。

検定  $T_n$  として、実数パラメータ  $a$  をもつ量子 Neyman-Pearson 検定

$$S_n(a) := \{\rho^{\otimes n} - e^{na}\sigma^{\otimes n} > 0\} \quad (14)$$

を考える。ここで、任意のエルミート行列  $A$  に対し、行列  $\{A > 0\}$  を以下のように定める<sup>\*1</sup>。  $A$  の固有値と固有ベクトルから成る正規直交基底をそれぞれ  $\{\lambda_i\}$ ,  $\{|x_i\rangle\}$  (縦ベクトル) とおくと、 $A$  のスペクトル分解

$$A = \sum_i \lambda_i |x_i\rangle \langle x_i| \quad (15)$$

が得られる。これに対し、

$$\{A > 0\} := \sum_{\lambda_i > 0} |x_i\rangle \langle x_i| \quad (16)$$

と定義する。すなわち、 $\{A > 0\}$  は  $A$  と同じサイズのエルミート行列であり、 $A$  の正固有値に対応する固有空間の直和への射影を表す。同様に、

$$\{A \leq 0\} := \sum_{\lambda_i \leq 0} |x_i\rangle \langle x_i| \quad (17)$$

も定義できる。ここで、

$$\{A > 0\} + \{A \leq 0\} = I$$

<sup>\*1</sup>  $\{A > 0\}$  という記法は、「確率変数  $A$  が正の値をとるという事象」の類似物として導入されたものである [2].

であるから, 集合  $\{\{A > 0\}, \{A \leq 0\}\}$  は POVM をなしていることに注意する.

量子 Neyman-Pearson 検定  $S_n(a)$  を用いたときの第 1 種・第 2 種誤り確率は式 (12), (13) より,

$$\begin{aligned}\alpha_n(a) &:= \alpha_n[S_n(a)] \\ &= \text{Tr}[\rho^{\otimes n} \{\rho^{\otimes n} - e^{na} \sigma^{\otimes n} \leq 0\}] = 1 - \text{Tr}[\rho^{\otimes n} \{\rho^{\otimes n} - e^{na} \sigma^{\otimes n} > 0\}]\end{aligned}\quad (18)$$

$$\begin{aligned}\beta_n(a) &:= \beta_n[S_n(a)] \\ &= \text{Tr}[\sigma^{\otimes n} \{\rho^{\otimes n} - e^{na} \sigma^{\otimes n} > 0\}]\end{aligned}\quad (19)$$

と表される.

第 1 種・第 2 種誤り確率  $\alpha_n(a), \beta_n(a)$  に対して, 以下が成り立つ.

**定理 1** (量子 Neyman-Pearson の補題 [11]). 任意の検定  $T_n$  と実数  $a$  に対して,  $\alpha_n[T_n] \leq \alpha_n(a)$  ならば  $\beta_n[T_n] \geq \beta_n(a)$  が成り立つ.

この定理は,  $\alpha_n[T_n]$  を  $\alpha_n(a)$  よりも小さく抑えようとすると, もう片方の  $\beta_n[T_n]$  が  $\beta_n(a)$  よりも大きくなってしまふことを主張している. この意味で, 量子 Neyman-Pearson 検定は最適な検定である.

## 5 量子仮説検定の漸近論

本節では, 第 1 種・第 2 種誤り確率  $\alpha_n[T_n], \beta_n[T_n]$  の  $n \rightarrow \infty$  における漸近的挙動に関するいくつかの事実を述べる [1, 2].

$n \rightarrow \infty$  における漸近的挙動については, 誤り確率そのものよりも,

$$-\lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha_n[T_n], \quad -\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n[T_n] \quad (20)$$

といった指数的な量に興味がある. ここで,

$$-\lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha_n[T_n] = R, \quad -\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n[T_n] = r \quad (21)$$

の関係が成り立っているとき,

$$\alpha_n[T_n] \sim e^{-nR}, \quad \beta_n[T_n] \sim e^{-nr} \quad (22)$$

というように  $\alpha_n[T_n]$  と  $\beta_n[T_n]$  を近似できることに注意する. また, 極限  $\lim$  を用いているが, 極限が存在するとは限らないので本来は  $\limsup, \liminf$  を使うべきである. しかし, 本稿では簡単のため極限  $\lim$  が存在すると仮定して議論をしていく.

第 1 種誤り確率  $\alpha_n[T_n]$  に指数的な制約を課した状況で, 第 2 種誤り確率  $\beta_n[T_n]$  の収束値に関して, 以下の定理が知られている. それについて述べるため, 量子相対エントロピー

$$D(\sigma \parallel \rho) := \text{Tr}[\sigma(\log \sigma - \log \rho)] \quad (23)$$

という量を導入しておく.

**定理 2** (量子 Stein の補題の順定理 [12]). 任意の  $R < D(\sigma \parallel \rho)$  に対して,

$$-\lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha_n[T_n] \geq R, \quad (24)$$

$$\lim_{n \rightarrow \infty} \beta_n[T_n] = 0 \quad (25)$$

を満たす検定の列  $\{T_n\}$  が存在する.

定理 3 (量子 Stein の補題の強逆定理 [13]).

$$-\lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha_n[T_n] > D(\sigma \| \rho) \quad (26)$$

ならば

$$\lim_{n \rightarrow \infty} \beta_n[T_n] = 1 \quad (27)$$

である.

式 (22) からわかるように,  $r$  や  $R$  は誤り確率が 0 に近づく指数的な速度であるから, 双方ともできるだけ大きくできることが望ましい. しかし,  $R, r$  は  $\alpha_n[T_n], \beta_n[T_n]$  と同様に, 片方を大きくすればもう片方が小さくなっていくというトレードオフの関係にある. そこで, 片方たとえば  $R$  に制約を課し,  $r$  の方を最大化することを考える. すなわち, 式 (24) をみたす検定  $\{T_n\}$  の中で, 式 (25) における  $\beta_n[T_n]$  の最大の収束指数

$$r := \max_{\{T_n\}} \left\{ -\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n[T_n] \mid -\lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha_n[T_n] \geq R \right\} \quad (28)$$

は次の定理で与えられる.

定理 4 (量子 Hoeffding の定理 [14–16]).  $R < D(\sigma \| \rho)$  のとき, 実数パラメータ  $a$  を用いて

$$r = r(a) = \max_{\theta \in \mathbb{R}} \{ \theta a - \psi(\theta) \} \quad (29)$$

$$R = R(a) = \max_{\theta \in \mathbb{R}} \{ (\theta - 1)a - \psi(\theta) \} = r(a) - a \quad (30)$$

と表される. この変換をルジャンドル変換と呼ぶ. ただし,

$$\psi(\theta) = \log \text{Tr}[\rho^\theta \sigma^{1-\theta}] \quad (31)$$

である. 式 (29), (30) の収束指数は, 式 (14) で定義した量子 Neyman-Pearson 検定  $S_n(a)$  で達成される.

## 6 $2 \times 2$ 行列のテンソル積の既約分解

以降では, 4 節で紹介した第 2 種誤り確率  $\beta_n(a)$  を数値計算の題材とする. この計算を行うには行列  $\rho^{\otimes n} - e^{na} \sigma^{\otimes n}$  を数値的に固有値分解する必要があるが, この行列のサイズは指数オーダーであり固有値分解は困難である. そこで, 表現論において知られている「テンソル積を重複する行列に直和分解できる」という既約分解 [17, 18] の手法を用いることにする. 本稿では  $2 \times 2$  の密度行列のみを扱うので, 本節ではこの場合について既約分解の詳細を述べる. (誤り確率の計算への応用は 7 節で述べる.)

各自然数  $n$  に対して  $2^n \times 2^n$  のユニタリ行列  $V$  が存在し, 任意の  $2 \times 2$  行列

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

に対し,  $VA^{\otimes n}V^*$  は

$$VA^{\otimes n}V^* = \bigoplus_{k=0}^{\lfloor n/2 \rfloor} \bigoplus_{m_k} A_k = \begin{bmatrix} A_0 & & & O \\ & A_1 & & \\ & & A_1 & \\ O & & & \ddots \\ & & & & A_{\lfloor \frac{n}{2} \rfloor} \end{bmatrix} \quad (32)$$

という形のブロック対角行列で表される. 各  $A_k$  はテンソル積  $A^{\otimes n}$  の既約成分<sup>\*2</sup>であり, そのサイズは  $\dim A_k = n + 1 - 2k$  で, 重複度  $m_k := {}_nC_k - {}_nC_{k-1}$  回だけ現れる. (ここで, 便宜的に  ${}_nC_{-1} := 0$  とする.) つまり, 式 (32) はまず  $A_0$  を  $m_0 = 1$  個だけ対角に並べ, 次に  $A_1$  を  $m_1$  個だけ対角に並べるという操作を繰り返して得られる  $\sum_k ({}_nC_k - {}_nC_{k-1})(n + 1 - 2k) = 2^n$  サイズの正方行列である. ここで, 式 (32) のユニタリ行列  $V$  は  $A$  に依らずに定まるという点が以下に述べる理由のため重要である. それは, 以下のように  $2 \times 2$  の行列  $A, B$  および実数  $a, b$  に対して, スカラー倍を伴う加算・乗算が既約成分ごとに行えることである:

$$V(aA^{\otimes n} + bB^{\otimes n})V^* = \bigoplus_{k=0}^{\lfloor n/2 \rfloor} \bigoplus_{m_k} (aA_k + bB_k) \quad (33)$$

$$V(A^{\otimes n} B^{\otimes n})V^* = \bigoplus_{k=0}^{\lfloor n/2 \rfloor} \bigoplus_{m_k} (A_k B_k). \quad (34)$$

ここで, 我々は行列のトレースを計算するために既約分解を用いるので, ユニタリ行列  $V$  そのものを求める必要はないことを注意しておく.

既約成分  $A_k$  の  $(i, j)$  成分  $\alpha_{k,ij}$  ( $i, j \in \{0, 1, \dots, r\}$ ) は以下のように求められる,  $r := n - 2k$  とし, まず

$$(a_{11}y + a_{21}z)^{r-j} (a_{12}y + a_{22}z)^j = \sum_{i=0}^r \alpha'_{k,ij} y^{r-i} z^i \quad (35)$$

という多項式展開から係数  $\alpha'_{k,ij}$  を求め, これを用いて

$$\alpha_{k,ij} = (\det A)^k \sqrt{\frac{{}_rC_j}{{}_rC_i}} \alpha'_{k,ij} \quad (36)$$

と計算できる.

例 (テンソル次数  $n = 2$  の場合). この場合,  $4 \times 4$  のユニタリ行列  $V$  が存在して,

$$VA^{\otimes 2}V^* = \begin{bmatrix} A_0 & O \\ O & A_1 \end{bmatrix}$$

とブロック対角化でき,  $\dim A_0 = 3, \dim A_1 = 1$  で,  $m_0 = m_1 = 1$  となり既約成分に重複はない.

まず, 既約成分  $A_0$  の行列成分  $[\alpha_{0,ij}]$  を求める. 式 (35), (36) より,

$$[\alpha'_{0,ij}] = \begin{bmatrix} a^2 & ab & b^2 \\ 2ac & ad + cb & 2bd \\ c^2 & cd & d^2 \end{bmatrix}$$

$$[\alpha_{0,ij}] = \begin{bmatrix} a^2 & \sqrt{2}ab & b^2 \\ \sqrt{2}ac & ad + cb & \sqrt{2}bd \\ c^2 & \sqrt{2}cd & d^2 \end{bmatrix}$$

と求められる.

次に, 既約成分  $A_1$  の行列成分  $[\alpha_{1,ij}]$  を求める. 既約成分  $A_0$  を求めるときと同様に,

$$[\alpha'_{1,ij}] = [1]$$

$$[\alpha_{1,ij}] = (\det A)[\alpha'_{1,ij}] = [ad - bc]$$

となる.

<sup>\*2</sup> 元来「既約成分」という言葉は, 行列  $A_k$  が作用する線形部分空間の呼称であるが, 本論文では行列  $A_k$  そのものを指す用語として用いる. 同様に, 「既約分解」という言葉も, 元来は  $A^{\otimes n}$  が作用する線形部分空間の直和分解の意味で用いられるが, 本論文では式 (32) そのものを表す用語として用いる.



## 7 テンソル積の既約分解を用いた誤り確率の計算

本節では、前節で述べたテンソル積の既約分解を誤り確率の計算に適用する。(以下では、第2種誤り確率  $\beta_n(a)$  の計算手順について述べるが、第1種誤り確率  $\alpha_n(a)$  についてもまったく同様である.)

式 (33),(34) より、誤り確率  $\beta_n(a)$  は次のように表される:

$$\beta_n(a) = \text{Tr}[\sigma^{\otimes n} \{\rho^{\otimes n} - e^{na} \sigma^{\otimes n} > 0\}] \quad (37)$$

$$= \sum_{k=0}^{\lfloor n/2 \rfloor} m_k \text{Tr}[\sigma_k \{\rho_k - e^{na} \sigma_k > 0\}]. \quad (38)$$

ただし、 $\{\rho_k\}$  と  $\{\sigma_k\}$  はそれぞれ  $\rho^{\otimes n}$  と  $\sigma^{\otimes n}$  の既約成分である。式 (38) で、

$$\beta_{n,k}(a) := \text{Tr}[\sigma_k \{\rho_k - e^{na} \sigma_k > 0\}] \quad (39)$$

とおくと、誤り確率  $\beta_n(a)$  は

$$\beta_n(a) = \sum_{k=0}^{\lfloor n/2 \rfloor} m_k \beta_{n,k}(a) \quad (40)$$

と表せる。図4で式 (39),(40) の計算手順を与える。

(ステップ) 1. 各  $k$  について、以下を行う。

(a) 式 (35),(36) を用いて  $\{\rho_k\}$  と  $\{\sigma_k\}$  を計算する。

(b) 行列  $\rho_k - e^{na} \sigma_k$  の固有値  $\{\lambda_{n,k,i}\}_i$  と正規直交化された固有ベクトル  $\{v_{n,k,i}\}_i$  を数値解法で求める。

(c)  $\beta_{n,k}(a) = \sum_{\lambda_{n,k,i} > 0} \langle v_{n,k,i} | \sigma_k | v_{n,k,i} \rangle$  を求める。

(ステップ) 2.  $\beta_n(a) = \sum_{k=0}^{\lfloor n/2 \rfloor} m_k \beta_{n,k}(a)$  を求める。

図4  $\beta_n(a)$  の計算手順

図4の手順のステップ1において各  $k$  に対する処理は独立なので、計算機実装する際には並列化を施している。また、ステップ1.(b)で固有値分解を行う行列の固有値は指数的にばらついているため、固有値分解の過程で大きな数値誤差が生じる。そのため、通常の数値計算で用いられる倍精度の桁数では足りないので、多倍長演算を用いることにする。

本研究では、密度行列  $\rho, \sigma$  は  $2 \times 2$  の場合に限るので、 $\rho, \sigma$  は実対称行列に限っても一般性を失わない。そのため、実際の計算では  $\rho, \sigma$  は実対称行列のみを扱う。行列  $\rho_k - e^{na} \sigma_k$  も実対称行列であるので、この固有値分解にも実対称行列向けのルーチンを用いる。

## 8 量子 Hoeffding の定理の数値的検証

本節では、前節で述べた既約分解を用いた誤り確率の計算法を使って、量子 Hoeffding の定理の数値的な検証を行う。

計算を行う値に対する用語や記号を整理しておく。密度行列  $\rho, \sigma$  を一組固定し、任意のテンソル次数  $n$  と実数  $a$  に対し、

$$r_n(a) := -\frac{1}{n} \log \beta_n(a) \quad (41)$$

$$r(a) := \lim_{n \rightarrow \infty} r_n(a) \quad (42)$$

とおく。ここで、 $r_n(a)$  を誤り指数、 $r(a)$  を極限值と呼ぶことにする。

我々は量子 Hoeffding の定理を数値的に検証するために、誤り指数  $r_n(a)$  と極限值  $r(a)$  の数値計算を行い、 $n$  が大きくなるにつれて  $r_n(a)$  が  $r(a)$  に近づいていく様子を観察する。なお、極限值  $r(a)$  は、定理 4 より表式 (29) がわかっている。ここで、式 (31) の  $\psi(\theta)$  は凸関数であるので、Newton 法を用いて簡単に式 (29) の最右辺の  $\max$  を計算できる。

用いる密度行列は

$$\rho = U\left(\frac{\pi}{4}\right)^* \begin{bmatrix} 0.1 & 0 \\ 0 & 0.9 \end{bmatrix} U\left(\frac{\pi}{4}\right), \quad \sigma = U\left(\frac{\pi}{6}\right)^* \begin{bmatrix} 0.95 & 0 \\ 0 & 0.05 \end{bmatrix} U\left(\frac{\pi}{6}\right) \quad (43)$$

である。ただし、

$$U(\theta) := \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \quad (44)$$

である。

この密度行列について、まず、いくつかの  $n$  に対して誤り指数  $r_n(a)$  と極限值  $r(a)$  を計算した結果を図 5 に示す。なお、本稿の図において、計算結果の曲線はスプラインを用いず折れ線で描画している。図 5 より、テンソル次数  $n$  を大きくしていくにつれて  $r_n(a)$  が  $r(a)$  に近づいていく様子が見て取れる。

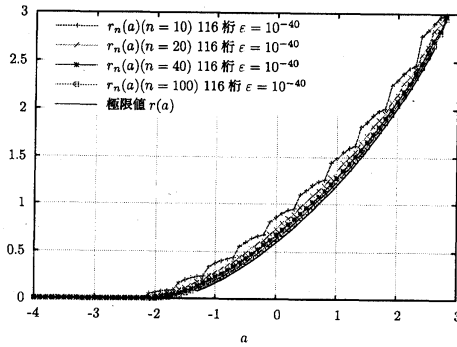


図 5 誤り指数  $r_n(a)$  が極限值  $r(a)$  に近づいていく様子

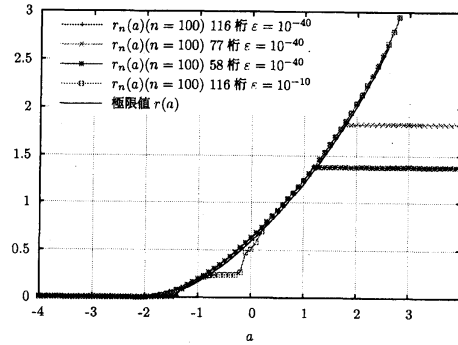


図 6 桁数や  $\varepsilon$  を変えたときの誤り指数  $r_n(a)$

次に、 $n = 100$  の場合の  $r_n(a)$  を桁数と  $\varepsilon$  を変えて計算した結果を図 6 に掲載する。図 6 において、桁数を 58, 77 桁と少なくした場合（青色・緑色のグラフ）は、それぞれ  $a = 1.3, 1.9$  以上でグラフが乱れ飽和するような現象が生じている。また、 $\varepsilon = 10^{-10}$  と甘い場合（桃色のグラフ）は  $a = -0.8 \sim 0.2$  あたりで乱れている。

このような歪は、他の  $\rho, \sigma$  でも起きることを確認している。理論的に  $r_n(a) > r(a)$  がわかっているので、誤り指数  $r_n(a)$  が極限值  $r(a)$  を下回っている箇所は数値誤差が原因である。

以上の考察より、本問題で精度の良い結果を得るには、多倍長演算が必要であることがわかった。誤り指数  $r_n(a)$  の乱れの主因は、指数的にばらついた行列を固有値分解する際の数値誤差であり、その数値誤差がどのように最終的な計算結果である誤り指数  $r_n(a)$  に現れるのかについての詳しい分析は文献 [6] で行っている。以上で、量子 i.i.d. 状態の数値計算手法が確立されたといえる。

## 9 新種の量子中心極限定理の数値的検証

前節では、既約分解を用いた量子 i.i.d. 状態の数値計算手法を確立するために、既に知られた量子 Hoeffding の定理を数値的に検証した。本節では、この計算手法を新しい数学的予想の数値的検証に適用し、その有効性を示す。

まず、新しい予想の問題設定を述べる。これまで、パラメータ  $a$  は  $n$  に依存しない定数としていた。ここでは、新たなパラメータ  $y \in \mathbb{R}$  を導入し、

$$a := -D(\sigma \parallel \rho) - \frac{y}{\sqrt{n}}$$

とおく。このとき、 $\beta_n(a)$  は

$$\gamma_n(y) := \text{Tr}[\sigma^{\otimes n} \{ \rho^{\otimes n} - \exp[-n(D(\sigma \parallel \rho) + \frac{y}{\sqrt{n}})] \sigma^{\otimes n} > 0 \}] \quad (45)$$

と表される。我々は、 $\gamma_n(y)$  の  $n \rightarrow \infty$  としたときの漸近的な振る舞いに興味がある。

古典論では、 $\gamma_n(y)$  は

$$\begin{aligned} \gamma_n(y) &= \Pr\{p^n(X^n) - \exp[-n(D(q \parallel p) + \frac{y}{\sqrt{n}})]q^n(X^n) > 0\} \\ &= \Pr\{\frac{1}{n} \sum_{t=1}^n \log \frac{p(X_t)}{q(X_t)} > -D(q \parallel p) - \frac{y}{\sqrt{n}}\} \end{aligned} \quad (46)$$

と表される。ここで、 $p, q$  は任意の確率分布で、その相対エントロピーは  $D(q \parallel p) := \sum_x q(x) \log \frac{q(x)}{p(x)}$  である。また、 $X^n = (X_1, \dots, X_n)$  は確率変数で、 $q$  の i.i.d. 拡張  $q^n$  に従っているとする。このとき、

$$A_t := \log \frac{p(X_t)}{q(X_t)}$$

は平均値が相対エントロピー  $D(q \parallel p)$  の実数値確率変数である。ここで、 $A_t$  の分散を  $s$  とすると、 $\frac{1}{\sqrt{n}} \sum_{t=1}^n (A_t - \mu)$  は中心極限定理より、漸近的に平均値 0、分散  $s$  の正規分布に従う。すなわち、

$$\gamma_n(y) \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y/s} \exp(-\frac{\alpha^2}{2}) d\alpha \quad (n \rightarrow \infty) \quad (47)$$

である。

古典版の式 (47) からの類推より、式 (45) の量子版の  $\gamma_n(y)$  の極限值について次のような予想を立てる。

予想 1 (新種の量子中心極限定理)。

$$\gamma_n(y) \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y/s} \exp(-\frac{\alpha^2}{2}) d\alpha =: \gamma(y) \quad (n \rightarrow \infty) \quad (48)$$

ここで、 $s^2 = \text{Tr}[\sigma(\log \sigma - \log \rho - D(\sigma \parallel \rho)I)^2]$  である。

この予想の量子仮説検定における意義はまだ明らかではないが、現時点では証明も反例も知られておらず成り立っているかどうかという数学的な興味を引き起こす。

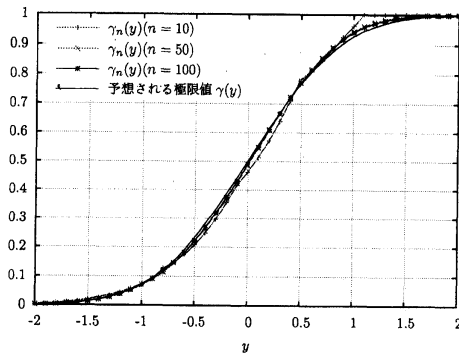
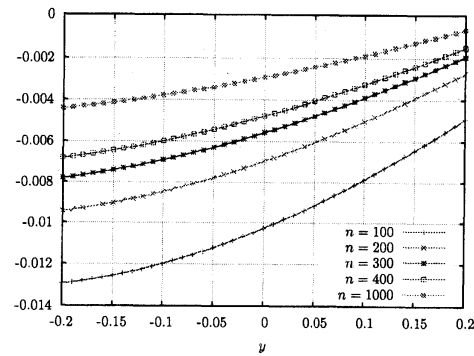
次に、既約分解を用いた誤り確率の計算アルゴリズムを使用して、この予想を数値的に検証する。シミュレーションで扱う密度行列は次の通りである：

$$\rho = U \left( \frac{\pi}{6} \right)^* \begin{bmatrix} 0.75 & 0 \\ 0 & 0.25 \end{bmatrix} U \left( \frac{\pi}{6} \right), \quad \sigma = \begin{bmatrix} 0.9 & 0 \\ 0 & 0.1 \end{bmatrix}. \quad (49)$$

信頼できる結果を得るため、計算はすべて多倍長演算で行う。また、計算にはスーパーコンピュータ 東京大学 HA8000 [19] を用いることにする。

図 7 に小さな  $n$  についてのシミュレーション結果を掲げる。図 7 において、 $\gamma_n(y)$  のグラフはほとんど  $\gamma(y)$  に重なっている。

収束していることを確かめるために、図 8 に大きな  $n$  について予想極限值との差  $\gamma_n(y) - \gamma(y)$  を掲げる。図 8 において、 $n$  が大きくなるほど、この差が 0 に近づいていく様子が観察できる。他の密度行列  $\rho, \sigma$  の組に関しても同様の収束を確認した。この結果は予想 1 の正しさを支持していると考えられる。

図7  $\gamma_n(y)$  と予想極限值  $\gamma(y)$ 図8 予想極限值との差  $\gamma_n(y) - \gamma(y)$ 

未知の極限定理の正答を数値シミュレーションによって調べることは、通常確率論においては常套手段となっているが、量子情報理論ではそのような研究例はほとんど報告されていない。本章で示した結果はそのような研究の有効性を示した一例であるといえる。

## 10 まとめ

本稿では、二つの量子 i.i.d. 状態に対する仮説検定問題を紹介した。また、この問題設定における誤り確率の計算にテンソル積の既約分解を適用した計算手法について述べた。以下は、この計算手法を用いて得られた結果である。

1. 量子 Hoeffding の定理を数値的に検証した。具体的には、テンソル次数  $n$  が大きくなるほど、誤り指数  $r_n(a)$  が極限值  $r(a)$  に収束していくことを確認した。
2. 新種の量子中心極限定理に適用し、予想した極限值に収束していくことを確かめた。

今後の課題としては、以下が考えられる。

3. 新種の量子中心極限定理の量子情報理論における意義を明らかにすること
4. 本稿では  $2 \times 2$  サイズの密度行列に対する量子 i.i.d. 状態を扱ったが、 $3 \times 3$  サイズ以上に拡張すること
5. 本稿では二つの量子 i.i.d. 状態に関する仮説検定問題を扱ったが、三つ以上の量子 i.i.d. 状態に拡張し、その漸近的性質を解明すること
6. 量子推定など他の問題への応用

## 謝辞

本研究を進めるにあたって、ご指導頂いた長岡浩司教授に感謝申し上げます。

平成 21 年度後期・22 年度前期の二度にわたってスパコン若手利用者推薦の支援をいただいた東京大学情報基盤センター・スーパーコンピューティング部門に謝意を表する。東京大学情報基盤センターには、平成 23 年度学際大規模情報基盤共同利用・共同研究拠点に際し、共同研究利用大学としても支援をいただいた。

最後に、RIMS 研究集会「量子論における統計的推測の理論と応用」で発表する機会を与えていただいた研究代表者の田中冬彦氏に感謝する。

## 参考文献

- [1] Masahito Hayashi. Asymptotics of quantum relative entropy from a representation theoretical viewpoint. *J. Phys. A: Math. Gen.*, Vol. 34, No. 16, pp. 3413–3419, 2001.
- [2] Hiroshi Nagaoka and Masahito Hayashi. An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses. *IEEE Trans. Inf. Theory*, Vol. 53, No. 2, pp. 534–549, 2007.
- [3] 柿崎晃. 量子的 i.i.d. 情報源に関する数値計算によるアプローチ. Master's thesis, 電気通信大学情報システム学研究科, 2006.
- [4] 堂嶋隆幸, 片桐孝洋, 長岡浩司. 量子 i.i.d. 状態における仮説検定の漸近特性に関する数値的アプローチ. 第 29 回情報理論とその応用シンポジウム予稿集 (SITA), pp. 767–770, 2006.
- [5] Tatsuya Sakashita and Hiroshi Nagaoka. A numerical study of hypothesis testing for quantum i.i.d. states. *Asian conference on quantum information science(AQIS)*, pp. 213–214, Aug. 2010.
- [6] 坂下達哉, 片桐孝洋, 長岡浩司. 量子 i.i.d. 状態の仮説検定に関する数値的手法とその誤差分析. 情報処理学会論文誌コンピューティングシステム (ACS), No. 35, October 2011.
- [7] 坂下達哉. 量子 i.i.d. 状態のシミュレーションとその理論的考察. スーパーコンピューティングニュース, Vol.13 特集号 1, , March 2011.
- [8] 坂下達哉, 長岡浩司. 量子 i.i.d. 状態のシミュレーションとその理論的考察. 日本応用数理学会 2010 年度年会 講演予稿集, pp. 245–246, 2010.
- [9] 坂下達哉. 量子 i.i.d. 状態の仮説検定問題における数値計算手法. 素粒子論研究・電子版, Vol. 13, No. 1, Sep 2012.
- [10] 坂下達哉. 量子 i.i.d. 状態に対する仮説検定の大規模シミュレーション. 統計関連学会連合大会講演報告集, p. 88, Sep 2012.
- [11] Alexander S. Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, Vol. 3, No. 4, pp. 337–394, December 1973.
- [12] Fumio Hiai and Dénes Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.*, Vol. 143, No. 1, pp. 99–114, December 1991.
- [13] Tomohiro Ogawa and Hiroshi Nagaoka. Strong converse and stein's lemma in quantum hypothesis testing. *IEEE Trans. Inf. Theory*, Vol. 46, No. 7, pp. 2428–2433, November 2000.
- [14] Tomohiro Ogawa and Masahito Hayashi. On error exponents in quantum hypothesis testing. *IEEE Trans. Inf. Theory*, Vol. 50, No. 6, pp. 1368–1372, June 2004.
- [15] Masahito Hayashi. Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding. *Phys. Rev. A*, Vol. 76, No. 6, pp. 062301–1, 062301–4, 2007.
- [16] Hiroshi Nagaoka. The converse part of the theorem for quantum Hoeffding bound. *arXiv:quant-ph/0611289v1*, 2006.
- [17] 山内恭彦, 杉浦光夫. 連続群論入門. 培風館, 2010.
- [18] 岩堀長慶. 対称群と一般線型群の表現論 (岩波講座 基礎数学). 岩波書店, 1978.
- [19] 東京大学情報基盤センター. HA8000 クラスタシステム. <http://www.cc.u-tokyo.ac.jp/system/ha8000/>.